Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

GUIDANCE ON RISK AND MITIGATION

FOR THE USE OF DRONES

RESEARCH SECURITY CENTRE

Uncrewed aerial systems (UAS), commonly referred to as drones, have become increasingly common tools in academic and applied research. Their ability to carry sensors, collect high-resolution data, and access areas that may be remote, hazardous, or difficult to reach has led to their adoption across a wide range of disciplines, including environmental science, ecology, archaeology, engineering, agriculture, public health, geosciences, and social sciences.

At the same time, the global market for drones and drone-enabled technologies has expanded rapidly. Researchers now have access to a growing number of commercially available platforms, manufacturers, and service providers operating across multiple jurisdictions. While this offers new opportunities, it also introduces new research security risks related to cybersecurity, privacy, data protection, and data sovereignty.

Data captured by drones can reveal sensitive information about the areas in which the drones are operating as well as the methods by which the drones are being used. If the drones are not procured from Canadian manufacturers or manufacturers in countries which have a trusted trading relationship with Canada, their connected components and associated peripherals may transfer this information to other jurisdictions with or without the user's awareness. Effort should also be made to ensure that the drones procured from Canadian and trusted sources are not "white-labeled" drones or contain components sourced from other jurisdictions. As such, the procurement and use of drones in research warrants additional due diligence and the implementation of appropriate mitigation measures to address these risks.

Canada

Researchers and research institutions are strongly encouraged to consider this guidance as they identify and mitigate risks associated with research involving drones, including when they complete Risk Assessment Forms as an integral part of grant applications that are subject to the National Security Guidelines for Research Partnerships.

RISKS

As per the established guidance from the Canadian Centre for Cyber Security (CCCS), the following are two important risk factors to be considered when working with drones:

DATA SECURITY

Drones are untrusted devices and can pose a significant risk to your organization when directly or indirectly connected to your network. Their connection can be leveraged by threat actors as an attack vector or used to gain remote access to your environment.

Some drones also require the use of cloud services to access encrypted flight metadata stored on the drone itself. If these cloud services are based outside Canada or a likeminded country, there is a strong possibility that the data collected from flight can be used by threat actors.

SATELLITE INTERFERENCE

Drones can be misled through satellite navigation interference by jamming or spoofing signals to create false signals and prevent communication with the drone. This can cause the user to completely lose control of the drone and can negatively impact the intended research results as well as create a hazard if the drones are being used in highly populated areas.

Prior to deploying a drone for their project, it is recommended that researchers work with their institution's IT security team and their research security office (where applicable) to conduct a risk assessment on the drone manufacturer and any potential cybersecurity and physical hazards that may be present in order to be well-positioned to mitigate those risks.

MITIGATION

Where possible, the Research Security Centre recommends that drones and their components from countries that do not have trusted trading relationships with Canada be avoided.

The best mitigation measure for these risks is to source drones and their associated peripherals from companies that manufacture them in Canada or from trusted trade partner countries.

Trusted vendors should incorporate secure-by-design and secure-by-default cybersecurity standards and should actively prioritize the security of their customers as a core business requirement.

Trusted vendors should also sell drones that are not "white-labelled" versions of drones from non-trusted sources and do not incorporate components from non-trusted sources.

Drones manufactured in countries that are trusted trade partners to Canada that do not incorporate such standards and practices pose similar data security risks as drones manufactured in countries that do not have trusted trading relationships with Canada.

In exceptional circumstances where drones cannot be procured from a trusted vendor, additional mitigation measures are highly recommended to appropriately address the associated research security and cyber security risks. These include, but are not limited to:

THE DRONE SHOULD BE CONTROLLED USING A DEDICATED OR STANDALONE CONTROLLER.

This controller must not be connected to any other device or network, except for the drone itself.

THE DRONE SHOULD BE USED IN OFFLINE MODE ONLY.

Most drone manufacturers allow individuals to use the drone and its related software in offline mode only. To do this effectively, all of the drone's settings must be switched to offline mode and you must ensure that all data that the drone is collecting is stored locally.

THE DRONE'S DATA MANAGEMENT SOFTWARE SHOULD BE USED EXCLUSIVELY IN OFFLINE MODE.

This can be done effectively by installing the drone manufacturer's software on a device that cannot be connected to the internet (for example: a laptop that has had its WiFi and Bluetooth chips removed).

- Many drone manufacturers require a cloud service to decrypt their data to access flight log metadata. If the servers for this cloud service are not located in Canada or likeminded countries, this information can be accessible to foreign security and intelligence services to the detriment of Canadian national security. Therefore, these services should not be used.

- If access to the drone's flight telemetry or metadata is required, the drone can instead be modified to install a third-party GPS module from a trusted provider which can provide information such as flight speed, height, and position, as needed.

MORE INFORMATION

For more information on cyber security considerations for drone use, you are encouraged to consult with Canadian cyber security experts. You may also consult the helpful guidance published by CCCS here.

If you have any project-specific questions relating to drones or drone mitigation, please do not hesitate to reach out to your institution's research security office or to the Research Security Centre directly.